THE GREAT MICROSOFT SECURITY RIP-OFF

MIP

A SOCIAL SOLUTION IN A DIGITAL DIMENSION

Covid-19 has shined an uncomfortably bright light on the state of cyber security around the world. As early as March 2020, Deloitte found that the pandemic led to increased security risk from remote working, delayed cyber-attack detection and response, gaps in physical and information security, and an influx of cybercriminals. Since the start of the pandemic, there has been a 300% increase in reported cybercrimes.

In addition, the increased popularity of crypto currency has enabled a larger community of cybercriminals to drive ransomware attacks. The ability to hide the ransom payment using unregulated currency has proven to be one of the key attributes of the crypto world being exploited by cybercriminals.

Despite the fact that the move to remote working increased the risk of cybercrime for companies of all sizes, their largest vulnerability is the fact that they use Microsoft as a platform for most things, says Richard Firth, CEO of MIP Holdings. "The vulnerabilities in various Microsoft products are the biggest source of cyber-attacks worldwide. Approximately 1.5 billion people use Windows operating systems every day, and the number of reported Microsoft vulnerabilities has risen a whopping 181% in the last five years. In 2020 alone, 1268 Microsoft vulnerabilities were discovered," he says.

"Many companies think that if they patch their software, they are fully secure. This is not the case. Several Microsoft issues may or may not receive a patch, and some are configuration issues that can't be patched. On GitHub, there is an entire 'won't fix' list of security issues that Microsoft has either not yet patched, won't patch, or are issues that need manual adjustment to fix."

Firth adds that many organisations are building a "Microsoft everything" strategy, by using Microsoft throughout their architecture. The logic is sound, he says. It is easier to use all the components that Microsoft have built to easily integrate into one delivery method, but now think about the ease by which a vulnerability can be spread throughout the organisation! This will increase the scope of a cyber-attack in the future, as cybercriminals continue to focus on the most widely used platform in the world.

"Most vulnerabilities are on Microsoft Exchange Servers, but all Microsoft products have been targeted by criminals. Check Point Research, for example, recently found four security vulnerabilities that affect products in the Microsoft Office suite, including Excel and Office online. Rooted from legacy code, the vulnerabilities create the potential for an attacker to execute code on targets via malicious Office documents, such as Word, Excel and Outlook."

As cyber-attacks continue to rise, and as they have a bigger impact on businesses and customers alike, companies will have to take a careful look at their choice of technologies, says Firth. "According to Ponemon's State of Cybersecurity Report, the long tail costs of a data breach can extend for months to years and include significant expenses that companies are not aware of or do not anticipate in their planning. These costs include lost data, business disruption, revenue losses from system downtime, notification costs, fines associated with government regulations designed to deal with breaches of 'Protection of Personal Information' or even damage to a brand's reputation," he explains.

> “ IN 2020 ALONE, 1268 MICROSOFT VULNERABILITIES WERE DISCOVERED

“Microsoft offers a ‘secure’ version of its products, at an additional cost. This would move a software development company such as MIP from a cost of U$20 per employee per month to a total cost of U$57 per employee per month. While many companies might see this as an investment in security, the fact that the secure version costs almost three times as much as the ‘normal’ version raises questions. There is no guarantee that the secure version will keep out all attackers – there isn’t a single product on the market that can do that – so additional tools will still be required. In fact, I would ask if this is any different to ‘Microsoft’ ransomware. Microsoft is charging almost triple for a product that will still require additional investment to secure, effectively taking advantage of their poor networking tooling to make extra money.”

Firth points out that some industries are more vulnerable to cyber-attacks than others, simply due to the nature of their business. While any industry could be subject to a data breach, those most at risk are businesses that are closely involved with people’s daily lives.

“Companies that hold sensitive data or personally identifiable information are common targets for hackers. These organisations have already invested heavily in their security, so why should they pay extra for a secure version of the tools that their businesses use daily? Shouldn’t the secure version be the standard version?” Firth asks.